

REMARKS

After the foregoing amendment, claims 1-19 are currently pending in this application.

Claim 14 has been amended to comport with claim 6. Claims 1, 2, 8, 10-12, and 14-18 have been amended to more distinctly claim subject matter which the applicants regard as the invention. Support is found at least in paragraph [0032], "... the destination address is looked up in the routing table or bit mask 144 of the routing device 112 to determine if the destination address is part of the same partition 116 as the source address... If the destination address is not found in the routing table or bit mask 144 the packet is not transmitted." In the specification, a sentence in paragraph [0032] has been amended to be more consistent with a preceding sentence of the same paragraph. Applicants submit that no new matter has been introduced into the application by this amendment.

Claim Rejections - 35 USC § 112

Claim 14 stands rejected under 35 USC § 112 second paragraph as being indefinite because a term therein does not have sufficient antecedent basis. Claim 14 has been amended as noted above. Support for the amendment is found at least in paragraph [0032] lines 16-18. Reconsideration and withdrawal of the 35 USC § 112 rejection of claim 14 are respectfully requested.

Claim Rejections - 35 USC § 102

Claims 1-4, 7-12, and 15-18 stand rejected under 35 USC § 102(e) as being allegedly anticipated by Green *et al.* (US 2004/0022257 A1). Applicants respectfully traverse this rejection.

It is well settled that a reference must teach every element or aspect of a claim in order to be considered prior art under 35 USC § 102(e). Green fails to do so.

The claims are drawn to preventing a computing element in one partition of a partitionable computer system from affecting any other partition in any way. In a computer system that has a packet routing function such as a crossbar, the highest levels of security and isolation in the routing function between unique entities is desired. A partition in such a computer system comprises the collection of computing elements on which operating systems and applications are run, including CPUs, memory, and I/O along with their support structure. The computing elements can connect to a fabric built upon crossbar switches that route packets from one element to another. By properly associating and configuring computing elements, many distinct partitions can be carved from the collection of elements, and the fabric provides for communication between the elements.

After the partitions are formed, it is critical that a computing element in any one partition be prevented from affecting any other partition in any way, even in rare conditions such as a defect in an element or a malicious user. The claims are directed to a hardware firewall built into the fabric crossbar switches that prevents one partition from sending packets to remote partitions. The firewall guarantees that an unauthorized packet can never be sent to a remote partition by confirming that the destination of every packet is in the same partition as the packet's source.

In contrast, Green pertains to a router that supports communications between separate subnets, managed by different subnet managers. The elements of a subnet have local identifiers (LIDs) specific to that subnet. The router makes end nodes from one subnet visible to another subnet. The same end node is identified by one local identifier (LID) value in one subnet, and by another LID in a different subnet. The router accepts from a first subnet packets directed to end nodes in a second subnet, and converts between the first and second LID values to provide for communication between subnets. (Green, Abstract.)

With regard to claim 1, claim 1 recites receiving a packet from a first partition, reading its destination address, determining if the packet destination is within the first partition, and if not, prohibiting the transmission of the packet. In contrast, Green teaches determining if the source

and destination addresses of a packet are in the same partition, and determining if they are allowed to communicate with each other. Thus, in Green the source and destination addresses of a packet may both be determined to be in the same partition, and they may be determined to not be allowed to communicate with each other, and the packet would be dropped whereas in claim 1 that packet would not be prohibited from being transmitted. Furthermore, in Green the source and destination addresses of a packet may be determined to be in different partitions, and they may be determined to be allowed to communicate with each other, and the packet would not be dropped whereas in claim 1 that packet would be prohibited from being transmitted. Although in Green it is possible that a packet with a destination in a remote partition would be dropped, it would not be dropped because the destination is in a remote partition, as in claim 1. Rather, it would be dropped because the destination is not allowed, presumably for some other reason.

Thus, Green is directed to facilitating communication between subnets, essentially the opposite of claim 1. Green does not teach or suggest that a packet be dropped because its destination address is in a remote partition, "prohibiting transmission of the packet to the destination address when the destination address is not within the first partition," as recited in claim 1. Therefore, claim 1 is deemed allowable over Green.

Independent claims 8 and 15 are directed to a system and a routing device, respectively, that also recite not sending the packet to the destination address if the destination address is not within the first partition. Therefore, those claims are also deemed allowable over Green. Claims 2-4 and 7 depend from claim 1, claims 9-12 depend from claim 8, and claims 16-18 depend from claim 15. Therefore, without prejudice to their own individual merits, those claims are also deemed allowable over Green.

Based on the arguments presented above, withdrawal of the 35 USC § 102(e) rejection of claims 1-4, 7-12, and 15-18 is respectfully requested.

Claim Rejections - 35 USC § 103

Claims 5, 6, 13, 14, and 19 stand rejected under 35 USC § 103(a) as being allegedly unpatentable over Green *et al.* (same as above) in view of Baehr *et al.* (US 5,884,025).

Applicants respectfully traverse this rejection.

Baehr is directed to a system for screening data packets transmitted between a protected network (such as a private network) and another network (such as a public network). The system includes connections to the private network, to the public network, and to a proxy network isolated from the private network. Packets into or out of the private network are received at the screen and filtered based on their contents, their state information, and other criteria including their source and destination. Actions are taken by the screen depending upon the determination of the filtering phase. The packets may be allowed through, altered, dropped, or directed to a host on the proxy network that performs functions of the intended destination. The passing through of packets without the addition of any network address pertaining to the screening system allows the screening system to function without being identifiable by such an address, thereby making it more difficult to target.

Like Green as discussed above, Baehr does not teach or suggest dropping a packet because its destination address is in a remote partition. Thus, neither Green nor Baehr, either alone or in any possible combination, teaches or suggests dropping a packet because its destination address is in a remote partition. Furthermore, adding that capability to Green and/or Baehr would not be obvious. Both Green and Baehr are directed to providing for communication between networks, subnetworks, and/or partitions. In contrast, the claims are directed to doing precisely the opposite, i.e., preventing any possibility that communication can occur between partitions. In the prior art, preventing any possibility of partitions communicating might be achieved simply by not providing a communication path between the partitions. However, the claims are directed to a partitionable computing system, wherein the partitions are formed from a collection of computing elements and a switching fabric. Furthermore, the partitions may be

reconfigured, such as by rearranging the computing elements among partitions, a process that includes reconfiguring the connections between elements. In such a system, it is not practicable to eradicate all possible communication paths between partitions. In spite of that, the claims provide a mechanism to ensure the partitions are completely isolated from each other.

It is noted that Beahr is relied on only for the additional features of claims 5, 6, 13, 14, and 19 over their parent claims. Claims 5 and 6 depend from claim 1, claims 13 and 14 depend from claim 8, and claim 19 depends from claim 15. Without prejudice to their own individual merits, those claims are deemed allowable over the cited references for at least the same reasons as their parent claims are allowable over Green alone.


Conclusion

In view of the foregoing amendment and remarks, applicants respectfully submit that the present application, including claims 1-19, is in condition for allowance and an early notice of allowance is respectfully requested.

Respectfully submitted,

MARK EDWARD SHAW, *et al.*

BY:


GREGORY J. LAVORGNA
Registration No. 30,469
Tel: 215-988-3309
Fax: 215-988-2757
Attorney for Applicant